(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 43 01 039 C 2**

(51) Int. Cl.[6]:
G 06 F 17/60
G 07 C 5/00

(21) Aktenzeichen: P 43 01 039.3-53
(22) Anmeldetag: 16. 1. 93
(43) Offenlegungstag: 21. 7. 94
(45) Veröffentlichungstag der Patenterteilung: 14. 6. 95

DE 43 01 039 C 2

(73) Patentinhaber:
Latsch, Uwe, Dipl.-Ing., 57074 Siegen, DE

(72) Erfinder:
gleich Patentinhaber

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

CH 6 49 399 A5

WEIMANN, Jürgen: Risiken und Sicherheitspotentiale der Chipkarte, in: Computer und Recht 12/1988, S. 1037-1041;

(54) Elektronisches System zur Verwaltung gemeinschaftlich genutzter Kraftfahrzeuge

(57) Die Verwaltung von gemeinschaftlich genutzten Kraftfahrzeugen (z. B. beim Car-Sharing) erfordert eine zuverlässige, nutzer- und reservierungsbezogene Kontrolle der Fahrzeugnutzung und eine automatische, manipulationssichere Erfassung aller für die Abrechnung relevanter Daten. Herkömmliche elektronische Fahrtenschreiber erfüllen diese Anforderungen nicht.

Über ein modifiziertes schnurloses Telefon ermöglicht das beschriebene Bordcomputersystem die gezielte reservierungsabhängige Freigabe von Fahrzeugen für einen bestimmten Nutzer. Der Zugang zu den Fahrzeugen wird durch Chipkarten und ein Infrarot-Interface geregelt. Nach Fahrtende werden die nutzer- und fahrzeugbezogenen Daten über das schnurlose Telefon zu einer Abrechnungsstelle übertragen. Alle Funktionen sind in dem Bordcomputersystem integriert.

Das System eignet sich zum Einsatz in beliebigen Fuhrparks, in denen die Fahrzeuge verschiedenen Fahrern zugeordnet werden und in denen eine detaillierte Abrechnung der Fahrzeugnutzung verlangt wird.

DE 43 01 039 C 2

Beschreibung

Die Erfindung betrifft ein elektronisches System, das eine kostengünstige, effektive Verwaltung gemeinschaftlich genutzter Kraftfahrzeuge ermöglichen soll.

In vielen Städten wurden in den letzten Jahren sogenannte Carsharing-Organisationen gegründet, die ihren Mitgliedern einen über das Stadtgebiet verteilten Fahrzeugpark zur stundenweisen Nutzung zur Verfügung stellen. Der Nutzer muß dabei nur für die tatsächlich gefahrenen Kilometer und die Nutzungszeit bezahlen. Carsharing ist für Wenigfahrer daher eine günstige Alternative zum eigenen PKW. Vor der Fahrt muß der Nutzer eine Reservierung des gewünschten Fahrzeugs bei einer Zentrale anmelden. Den Fahrzeugschlüssel erhält er mit Hilfe eines Generalschlüssels aus einem Tresor am Fahrzeugstandort. Nach der Fahrt werden die Daten vom Nutzer in ein Fahrtenbuch eingetragen, dessen Auswertung die Abrechnung ermöglicht.

Probleme, die bei der Organisation auftreten sind:

— keine Kontrolle der tatsächlichen Fahrzeugnutzung, da jeder Nutzer uneingeschränkten Zugang zu den Fahrzeugen hat
— fehlerträchtige und manipulationsgefährdete Datenerfassung
— hoher Verwaltungsaufwand für Nutzer und Betreiber

Stand der Technik sind elektronische Fahrtenschreiber, Taxameter und Fuhrpark-Management-Systeme, die jedoch für diese Anwendung nicht geeignet sind, da diese:

— keine Zugangskontrolle zu den Fahrzeugen ermöglichen
— keine individuelle Nutzeridentifikation ermöglichen
— keine Datenverbindung zur Zentrale besitzen

Aus Patent CH 649 399 A5 ist eine "Anlage zum Reservieren von Dienstleistungen einer entfernten Dienstleistungsanordnung" bekannt. Sie betrifft jedoch lediglich das Reservierungsproblem, das bei der Verwaltung gemeinschaftlich genutzter Kraftfahrzeuge bereits hinreichend gelöst ist.

Die prinzipiellen Verfahren zur Authentikation in einer beliebigen Sicherheitsanwendung (Chipkarte und kryptographische Algorithmen) sind z. B. in dem Artikel "Risiken und Sicherheitspotentiale der Chipkarte" (Computer und Recht, 12/1988, S. 1037—1041) beschrieben. Sie werden auch als Sicherheitsmechanismus in der erfindungsgemäßen Anordnung zur Verwaltung gemeinschaftlich genutzter Kraftfahrzeuge eingesetzt.

Der Erfindung liegt die Aufgabe zugrunde, eine effektive, kostengünstige und manipulationssichere Verwaltung gemeinschaftlich genutzter Kraftfahrzeuge (Carsharing) zu ermöglichen. Die Aufgabe wird durch ein fahrzeuggebundenes System mit den Merkmalen des Patentanspruchs gelöst.

Die Erfindung wird anhand von Zeichnungen näher erläutert. Es zeigen:

Fig. 1 Ein Blockschaltbild des Gesamtsystems,

Fig. 2 Ein Blockschaltbild der Übertragungseinrichtung,

Fig. 3 Ein Blockschaltbild des Aufbaus der Infrarot-Chipkarten-Schnittstelle.

In **Fig.** 1 wird die erfindungsgemäße Anordnung durch ein vereinfachtes Blockschaltbild erläutert.

Die vier wesentlichen Grundgedanken sind:

1. Die drahtlose Sprach- und Datenkommunikation zwischen Zentrale und Fahrzeug über ein modifiziertes schnurloses Telefon,
2. Die Nutzeridentifikation über multifunktionale Mikroprozessor-Chipkarten,
3. Die Zugangskontrolle über eine Infrarot-Chipkarten-Schnittstelle (Wegfall des Standorttresors),
4. Die Steuerung des Gesamtsystems über einen einzigen Mikroprozessor.

Der Nutzer klärt die Reservierung wie bisher telefonisch mit der Zentrale (1). Ein Rechner (2) mit einem Reservationsprogramm übernimmt die Koordinierung der Reservierungen und übermittelt anschließend die Nutzerdaten mit Hilfe eines gängigen Modems (3) über das Telefonnetz (5) bis zur Feststation (7) eines schnurlosen Telefons in der Nähe des Standorts (6). Über die Funkstrecke des schnurlosen Telefons gelangen die Daten zum Mobilteil (12) im reservierten Fahrzeug (8) und werden dort gespeichert. Das Modem (13) und die Anwahlschaltung (14) werden zusätzlich in das Mobilteil (12) eingebaut.

Das schnurlose Telefon ist für diese Anwendung sehr gut geeignet, da es eine kostengünstige, individuelle Kommunikation mit jedem Fahrzeug ermöglicht. Die Einschränkung, daß das Fahrzeug nur im Umkreis von ca. 300 m um die Feststation erreichbar ist, ist unbedeutend, da das Fahrzeug nur an seinem Standort erreichbar sein muß.

Zum Öffnen des Fahrzeugs muß der Nutzer (21) seine persönliche Chipkarte (23) in das Infrarot-Handgerät (22) einführen. Über die Infrarotstrecke können Chipkarte (23) und Prozessor (20) im Fahrzeug miteinander kommunizieren. Nach Prüfling der Rücksetzantwort der Chipkarte (nachfolgend gemäß dem engl. Sprachgebrauch abkürzend als ATR (Answer to Reset) bezeichnet), sendet der Prozessor (20) den Befehl zum Öffnen der Zugangskontroll-Applikation zur Chipkarte. Die persönliche Identifikationsnummer (nachfolgend gemäß dem engl. Sprachgebrauch abkurzend als PIN (Personal Identification Number) bezeichnet) ist für diese Applikation bei allen Karten dieselbe und kann somit direkt vom Prozessor (20) zur Karte (23) übertragen werden. Das Infrarot-Handgerät (22) kommt daher ohne Tastatur aus. Die Zugangsberechtigung wird mittels eines auf der Chipkarte implementierten kryptographischen Algorithmus (z. B. Data Encryption Standard) überprüft. Hierzu sendet das Fahrzeugsystem eine Zufallszahl per Infrarotübertragung zur Chipkarte. Die Karte führt die entsprechende Verschlüsselung durch und sendet die Antwort zurück. Nur bei richtiger Antwort wird die Zentralverriegelung (10) des Fahrzeugs geöffnet. Ein Abhören der Übertragung kann nicht zum illegalen Öffnen des Fahrzeugs verwendet werden, da jedem Öffnungsvorgang eine andere Zufallszahl zugrunde liegt. Zusätzlich kann auch die auf der Karte gespeicherte Nutzeridentität abgefragt werden, um nur den Personen, die nicht in einer Sperrliste im Fahrzeug gespeichert sind, den Zugang zu ermöglichen.

Die eigentliche Nutzeridentifikation erfolgt erst im Fahrzeuginnern. Hier muß der Nutzer seine Chipkarte (23) in den Kartenleser (15) einführen und die richtige PIN auf der Tastatur (19) eingeben. PIN und Applikation sind hierbei verschieden zur Zugangskontrolle. Ein unberechtigtes Abhören der IR-Übertragung ermög-

licht daher nicht das Ausspähen der für die Nutzeridentifikation erforderlichen PIN. Die auf der Karte gespeicherte Nutzerkennung besteht aus der Nutzernummer und einem daraus mit einem geheimen Schlüssel berechneten Nachrichtenauthentikationscode (nachfolgend gemäß dem engl. Sprachgebrauch abkürzend als MAC (Message Authentikation Code) bezeichnet, der das Fälschen der Nutzernummer verhindern soll. Nur wenn PIN und MAC korrekt sind und eine Reservierung des aktuellen Nutzers für den momentanen Zeitraum vorliegt, wird die Zündung (11) freigegeben und der Fahrzeugschlüssel aus seiner mechanischen Verriegelung (9) gelöst.

Während der Fahrt werden die gefahrenen Kilometer über einen Tachosensor (16) erfaßt und in einem batteriegepufferten Speicher (18) abgelegt. Über entsprechende Sensoren können auch weitere Daten erfaßt werden.

Die Fahrt wird vom Nutzer durch Betätigung einer Taste beendet. Das Fahrzeugsystem prüft, ob sich das Fahrzeug an seinem Standort befindet, indem es die Empfangskennung des schnurlosen Telefons abfragt. Anschließend erfolgt mittels der Anwahlschaltung (14) eine automatische Anwahl der Zentrale (1) mit nachfolgender Übertragung von Nutzernummer und gesammelten Daten. Über eine Umschaltung des Mobilteils (12) des schnurlosen Telefons auf Sprachübertragung können evtl. aufgetretene Schäden direkt aus dem Fahrzeug einem Telefon (4) in der Zentrale mitgeteilt werden. Ein Abrechnungsprogramm in der Zentrale erstellt anhand der übertragenen Daten automatisch eine Rechnung.

Fig. 2 zeigt in einem Blockschaltbild die Veränderungen am Mobilteil (12) des schnurlosen Telefons, die eine Datenübertragung ermöglichen. Ein Teil der erforderlichen Bausteine (Decoder (37) und Analogschalter (38)) werden zwecks Einsparung von Kabeln in die Akku-Box des schnurlosen Telefons eingebaut. Als Modem (32) können alle handelsüblichen Telefon-Modem-Bausteine verwendet werden. Der Modulatorausgang (33) wird über einen Umschaltkontakt eines Relais (28) direkt an den NF-Verstärker (29) des schnurlosen Telefons angeschlossen, der das Signal zum HF-Teil (30) weiterleitet. Das Relais (28) ermöglicht das prozessorgesteuerte Umschalten zwischen Mikrofon (31) (Sprachübertragung) und Modulatorausgang (33) (Datenübertragung). Der Demodulatoreingang (34) ist direkt an den NF-Empfangsverstärker (35), parallel zum Lautsprecher (36), geschaltet. Die Datenübertragung erfolgt über die serielle Schnittstelle (25) des Mikroprozessors (24).

Die Anwahlschaltung (14) besteht aus einem 4-zu-16-Decoder (37) und 16 Analogschaltern (38), die parallel zum Tastaturfeld (39) des Telefons geschaltet sind. Über 4 Datenleitungen können so 16 Tasten des Telefons vom Prozessor (24) gesteuert werden. Zusätzlich werden dem Prozessor (24) das Anrufsignal (27) und die Empfangsbereichskennung (26) zugeführt. Hierdurch wird die automatische Beantwortung ankommender Rufe und die Standorterkennung ermöglicht.

Das Datenübertragungsprotokoll muß eine fehlerfreie Übertragung gewährleisten. Weder die zeitweise stark verrauschte Übertragungsstrecke noch der Ausfall der Verbindung während des Kenncodes des schnurlosen Telefons (alle 15 s für ca. 200 ms) dürfen Fehler verursachen. Hierfür sind alle gängigen Block-Protokolle mit CRC-Überwachung und Blockfolgesteuerung geeignet.

Fig. 3 zeigt den Aufbau der Infrarot-Chipkarten-Schnittstelle (17) und des IR-Handgerätes (22). Sie dienen dazu, dem Nutzer einen Zugang zum Fahrzeug mit Hilfe einer kontaktbehafteten Chipkarte (23) zu ermöglichen, ohne Veränderungen am Äußeren des Fahrzeugs (Einbau einer Kontaktiereinheit) vornehmen zu müssen. Nach Einschieben der Chipkarte (23) in die Kontaktiereinheit (41) des Handgeräts (40) und durch Betätigung des Tasters (47) wird die Spannungsversorgung (42) und der Taktgenerator (48) eingeschaltet. Die Datenleitung (45) der Chipkarte wird auf logisch "1" gelegt und die Karte wird mit dem Systemtakt (44) versorgt. Da die Empfangsdiode (55) im Handgerät kein Signal empfangt, wird über die Trägererkennung (52) des Frequenzumtast-Demodulators (54) (nachfolgend gemäß dem engl. Sprachgebrauch abkürzend als FSK-Demodulator bezeichnet) der Sendetreiber (50) durchgeschaltet und das vom FSK-Modulator (49) mit der Frequenz f_{H1} modulierte Signal über die Sendediode (53) ausgesendet. Das System im Fahrzeug (56) befindet sich zu dieser Zeit in einem stromsparenden Betriebszustand. Nur der FSK-Demodulator (64) ist eingeschaltet. Dieser schaltet aufgrund des an der Empfangsdiode (65) ankommenden Signals mit der Trägerkennung (61) über eine Einschaltlogik (60) den Prozessor (57) ein. Der Sendetreiber (58) im Fahrzeug wird gesperrt. Nach einer durch eine Verzögerungsschaltung (46) bestimmten Zeitverzögerung wird im Handgerät ein Rücksetzen (43) der Chipkarte ausgelöst. Die Karte antwortet mit dem ATR (Answer to Reset), dessen Bitfolge mit den Frequenzen f_{H1} und f_{H0} frequenzmoduliert über die Infrarot-Strecke zum Fahrzeug übertragen wird. Ist die vollständige Meldung im Fahrzeug angekommen, schaltet der Prozessor (57) den Sendetreiber (58) im Fahrzeug ein und ein Signal mit der Frequenz f_{F1} wird über die Sendediode (62) ausgesendet. Der FSK-Demodulator (54) im Handgerät erkennt den Träger und deaktiviert den Sendetreiber (50) im Handgerät. Gleichzeitig wird der FSK-Demodulator (54) über den Empfangstreiber (51) auf die Datenleitung (I/O) (45) der Chipkarte geschaltet. Nun kann der Prozessor (57) einen mit den Frequenzen f_{F1} und f_{F0} modulierten Befehl über die serielle Schnittstelle (63) zur Chipkarte senden. Nach dem Aussenden wird der Sendetreiber (58) im Fahrzeug wieder ausgeschaltet und die Übertragungsrichtung kehrt sich somit wieder um. Der FSK-Modulator (49) im Handgerät sendet in einem hohen Frequenzbereich mit den Frequenzen f_{H1} und f_{H0}, der FSK-Modulator (59) im Fahrzeug sendet in einem tieferen Frequenzbereich mit den Frequenzen f_{F1} und f_{F0}. Eine Störung der Umschaltung der Übertragungsrichtung durch Reflexionen an Fahrzeugteilen (Scheiben, Spiegel, Lack) wird so vermieden.

Die Eigenschaften des erfindungsgemäßen Systems lassen sich somit wie folgt kurz zusammenfassen:

— Wegfall des bisher benötigten Standorttresors durch ein kryptographisch geschütztes Infrarot-Zugangskontrollverfahren mit kontaktbehafteten, multifunktionalen Mikroprozessor-Chipkarten.

— Überwachung der Fahrzeugnutzung durch individuelle Nutzeridentifikation, Reservierungskontrolle und Fahrdatenerfassung.

— kostengünstige bidirektionale Daten- und Sprachverbindung zur Übertragung von Reservierungsdaten und Fahrdaten zwischen Zentrale und Fahrzeug am Standort.

Patentanspruch

Ein fahrzeuggebundenes System zur Reservierung, Zugangskontrolle, Nutzeridentifikation und Fahrdatenerfassung gemeinschaftlich genutzter Kraftfahrzeuge, wie z. B. beim Carsharing, **dadurch gekennzeichnet,**

— daß eine von einem Mikroprozessor gesteuerte bidirektionale Daten- und Sprachübertragung zur Übermittlung von Reservierungsdaten und Fahrdaten zwischen Fahrzeug und Zentrale mittels eines schnurlosen Telefons stattfindet, wobei das im Fahrzeug installierte Mobilteil (12) des schnurlosen Telefons durch einen Modembaustein (13) und eine prozessorgesteuerte Anwahlschaltung (14) und ein Umschaltrelais (28) ergänzt wird, während auf Seite der Zentrale ein handelsübliches Modem (3) eingesetzt wird und

— daß eine kryptographisch geschützte Zugangskontrolle über eine bidirektionale Infrarot-Kommunikation zwischen einer in ein Infrarot-Handgerät (22) eingeführten kontaktbehafteten multifunktionalen Mikroprozessor-Chipkarte (23) und einer Infrarot-Schnittstelle (17) im Fahrzeugsystem stattfindet, die bei richtiger Authentikation der Chipkarte die Zentralverriegelung (10) des Fahrzeugs öffnet, wobei das Einschalten des Fahrzeugsystems und die Umschaltung der Übertragungsrichtung im Handgerät durch die Trägerkennung (61 bzw. 52) zweier FSK-Demodulatoren (64 bzw. 54) realisiert wird und die Chipkarte über eine gesonderte Applikation zur Authentikation der Karte durch Verschlüsselung der vom Fahrzeugsystem gesendeten Zufallszahlen verfügt und

— daß im Fahrzeuginnern eine Nutzeridentifikation über eine andere Applikation derselben multifunktionalen Mikroprozessor-Chipkarte abgewickelt wird, die im Gegensatz zur Zugangskontroll-Applikation durch eine individuelle PIN abgesichert ist und die — bei Übereinstimmung der Nutzerdaten und der aktuellen Zeit mit den empfangenen Buchungsdaten — den Fahrzeugschlüssel aus einer mechanischen Verriegelung (10) löst und die Zündung (11) freigibt, wobei die Echtheit der auf der Karte gespeicherten Nutzernummer über einen zusätzlich auf der Karte gespeicherten Nachrichtenauthentikationscode (MAC) geprüft wird.

Hierzu 3 Seite(n) Zeichnungen

Numm
Int. Cl.[6]: G 06 F 17/60
Veröffentlichungstag: 14. Juni 1995
DE 43 01 039 C2

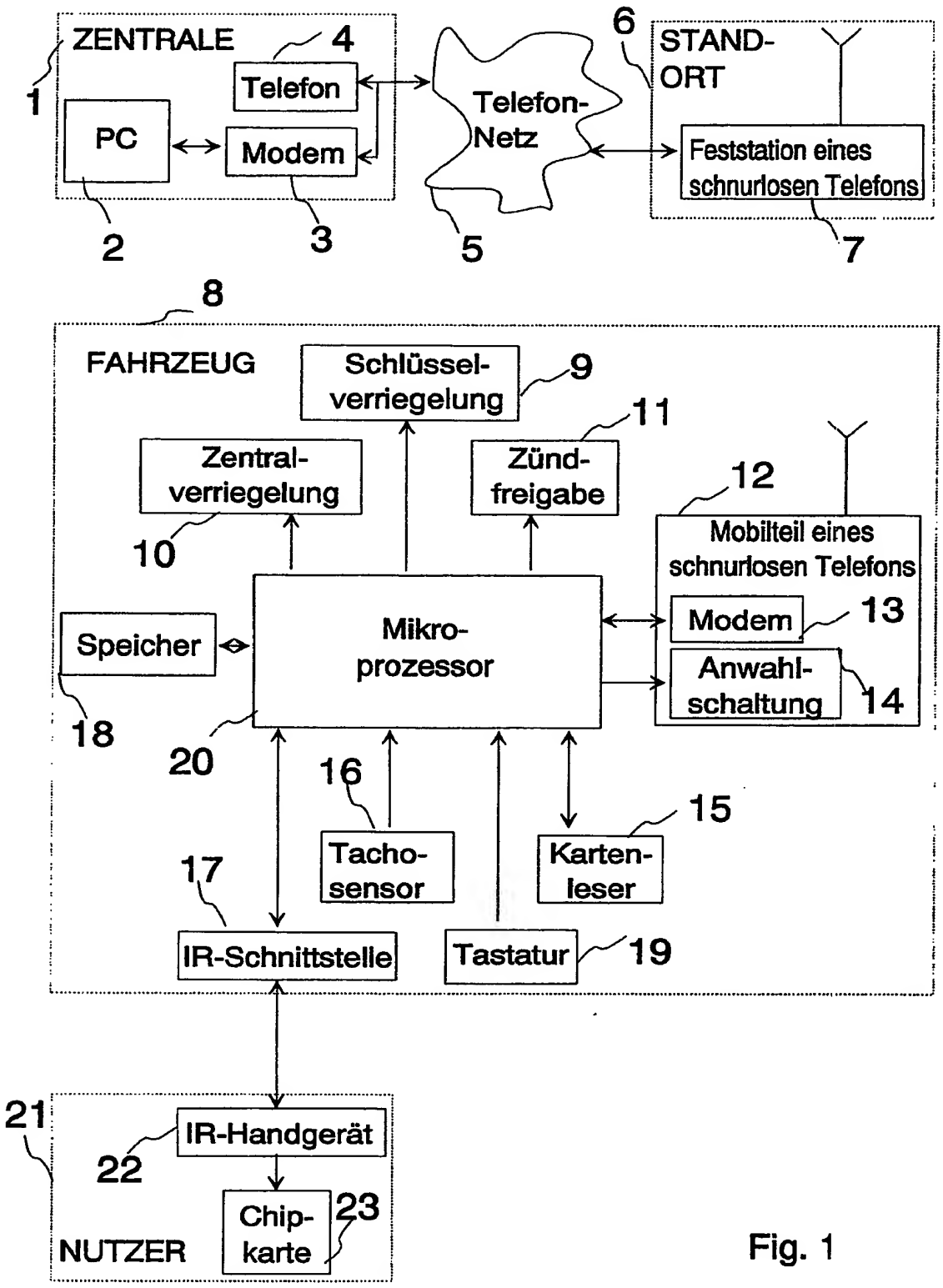


Fig. 1

Numm
Int. Cl.[6]: G 06 F 17/60
Veröffentlichungstag: 14. Juni 1995
DE 43 01 039 C2

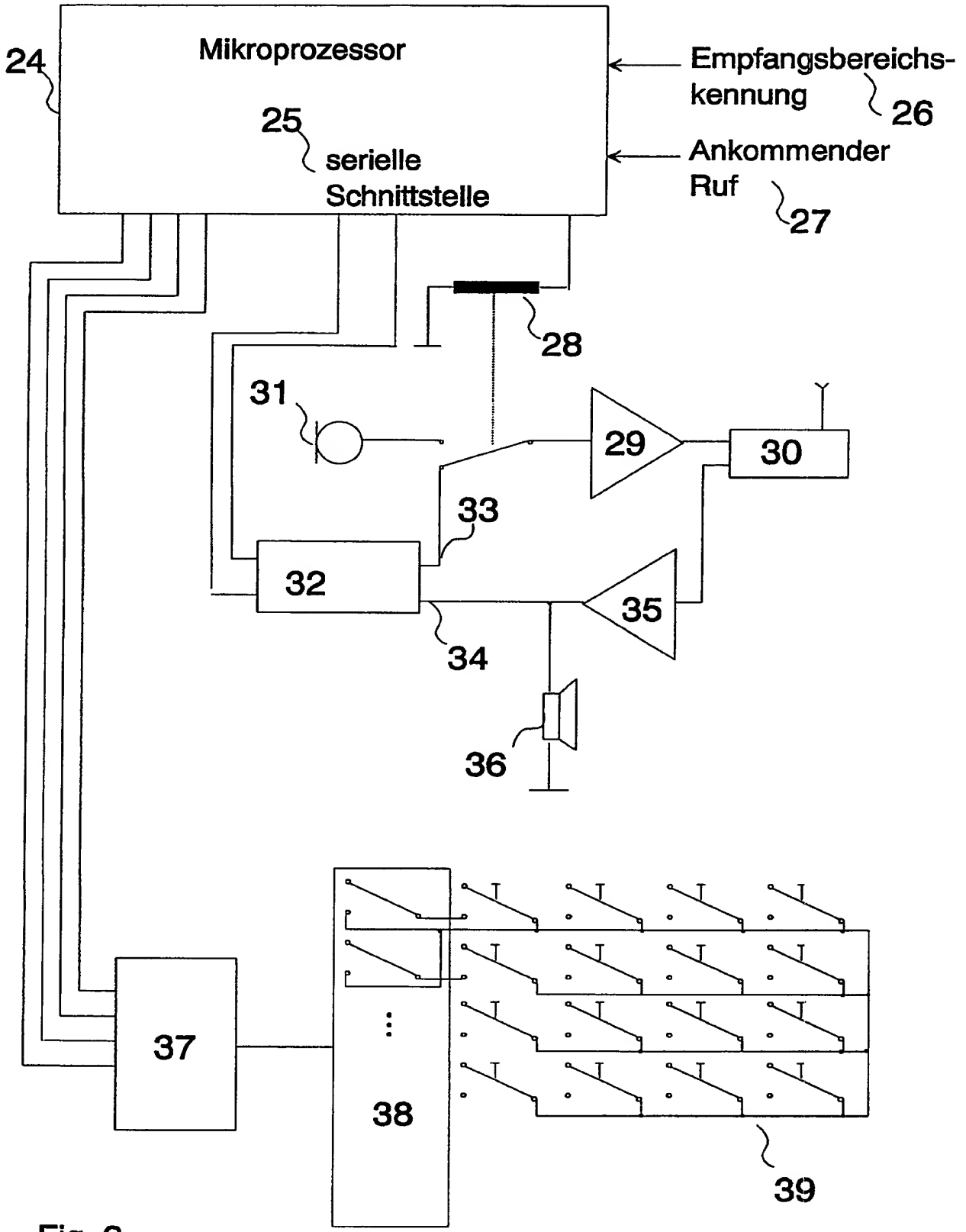
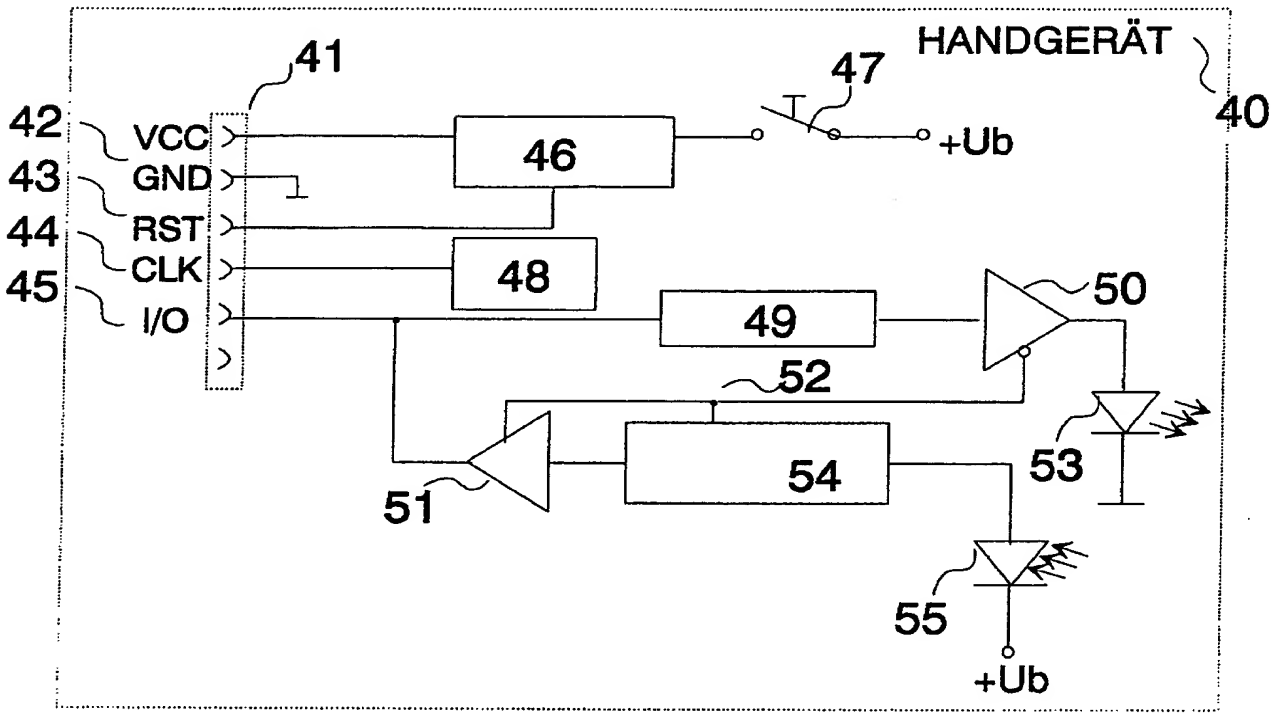


Fig. 2

Numm
Int. Cl.[6]:
Veröffentlichungstag:
DE 43 01 039 C2
G 06 F 17/60
14. Juni 1995



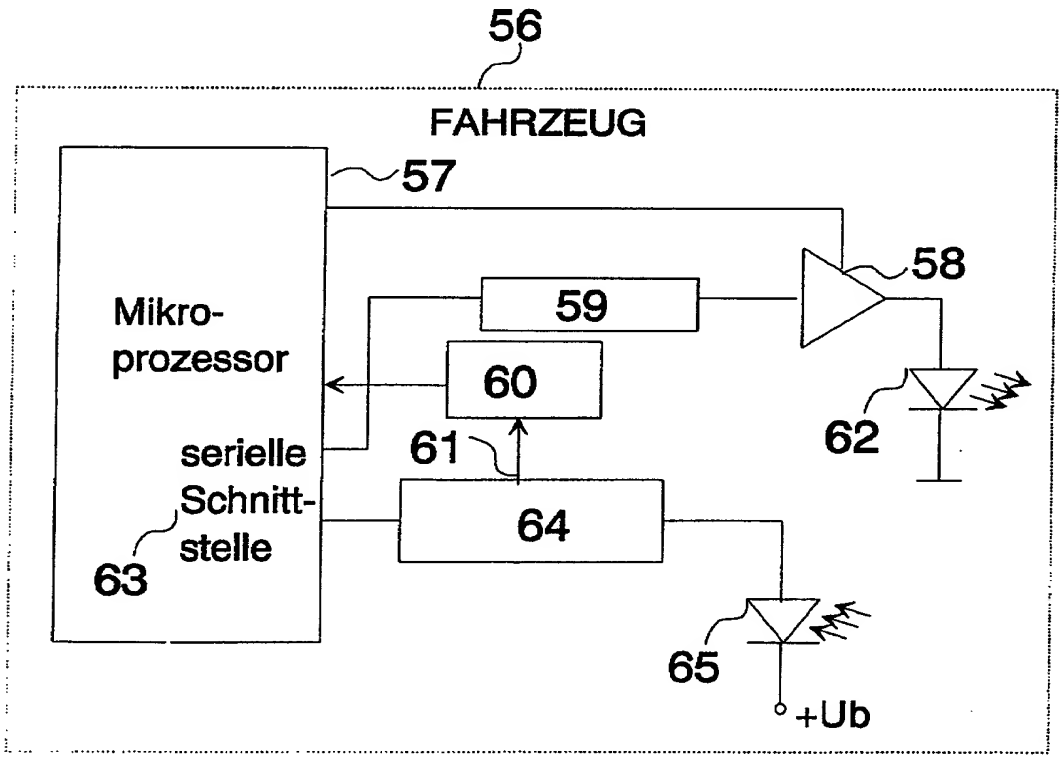


Fig. 3